UNITED STATES DISTRICT COURT
DISTRICT OF EASTERN VIRGINIA

CLIFFORD BEERS and WADE NUGENT, individually and on behalf of all others similarly situated, Plaintiff, v. **MAXIMUS, INC. and MAXIMUS FEDERAL SERVICES, INC.,** Defendants.	Civil Action No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Clifford Beers and Wade Nugent ("Plaintiffs"), individually and on behalf of themselves and all others similarly situated, allege the following against Maximus, Inc. and Maximus Federal Services, Inc. ("MFSI") (collectively "Maximus" or "Defendants"). The following allegations are based upon Plaintiffs' personal knowledge with respect to themselves and their own acts, and on information and belief as to all other matters.

I. INTRODUCTION

1. Plaintiffs and Class Members bring this class action against Maximus for its failure to properly secure and safeguard Plaintiffs' and similarly situated individuals' personally identifiable information ("PII") and protected health information ("PHI")—as defined by the Health Insurance Portability and Accountability Act ("HIPAA")—including but not limited to names, mailing addresses, dates of birth, Social Security numbers, Individual Taxpayer Identification numbers, telephone numbers, email addresses, driver's license numbers and state identification numbers, health benefit and enrollment information, and medical information

including medical records, conditions, diagnoses, treatments, images, and prescription information.

2. Maximus is a provider of health and human services that contracts with federal, state, and local entities to manage and administer government programs. Maximus touts itself as the "market leader in health services," having served 52 million Medicaid and Children's Health Insurance Program ("CHIP") beneficiaries and operating 72 state and local health programs. Maximus's business portfolio includes a contract with the Centers for Medicare & Medicaid Services ("CMS") to run its health insurance eligibility appeals process. Through these contracts, Maximus cumulatively possesses and stores the PII and PHI of millions of people in its databases.

3. This class action is brought on behalf of all citizens of all states in the United States who are the victims of a targeted cyberattack on Maximus that occurred on or before May 27, 2023 ("the Data Breach").

4. On or before May 27, 2023, Maximus allowed a cyber attacker to access and obtain the PII and PHI of Plaintiffs and Class Members.

5. On July 28, 2023, Maximus sent a letter of notice of the Data Breach ("Notice") to Plaintiffs via mail. That Notice failed to provide basic details concerning the Data Breach, including, but not limited to, how unauthorized parties accessed the Class Members records, whether the information was encrypted or otherwise protected, whether the breach was a system-wide breach, and how many people were affected by the Data Breach.

6. The Notice also failed to provide details on how many people were affected by the Data Breach—a number that continues to grow based on Maximus's ongoing disclosures. On July 26, 2023, Maximus stated it estimated that the Data Breach impacted "at least 8 to 11 million

individuals to whom the Company anticipates providing notice of the incident."[1] Then, on August 3, 2023, Maximus increased that estimate to be "at least 14.5 to 17.5 million individuals to whom the Company anticipates providing notice of the incident."[2] Based on these disclosures, millions of impacted victims were not notified of the Data Breach within the 60 days required by law.

7. Maximus knowingly collected individuals' PII and PHI (collectively, "Private Information") in confidence, and has a resulting duty to secure, maintain, protect, and safeguard that Private Information against unauthorized access and disclosure through reasonable and adequate security measures.

8. PHI is considered "the most confidential and valuable type of [PII] . . . irrevocable once breached."[3]

9. As a result of the Data Breach, Plaintiffs and Class Members suffered ascertainable losses, including, but not limited to, a loss of potential value of their private and confidential information, the loss of the benefit of their contractual bargain with Maximus, out-of-pocket

[1] Maximus Inc. (Form 8-K) (July 26, 2023).

[2] Maximus Inc., Form 10-Q (Aug. 3, 2023).

[3] Junyuan Ke, et al., *My Data or My Health? Heterogenous Patient Responses to Healthcare Data Breach*, SSRN (Feb. 10, 2022), http://dx.doi.org/10.2139/ssrn.4029103. Under the Health Insurance Portability and Accountability Act, 42 U.S.C. §§1320d, et seq. ("HIPAA"), PHI is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. §160.103. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. Summary of the HIPAA Privacy Rule, U.S. DEP'T OF HEALTH & HUMAN SERS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited Aug. 17, 2023).

expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

10. Plaintiffs and Class Members entrusted their Private Information to Maximus, its officials, and agents. That Private Information was subsequently compromised, unlawfully accessed, and stolen due to the Data Breach.

11. Plaintiffs bring this class action lawsuit on behalf of themselves and all others similarly situated to address Maximus's inadequate safeguarding of Plaintiffs' and Class Members' Private Information, for failing to provide adequate notice to Plaintiffs and other Class Members of the unauthorized access to their Private Information by a cyber attacker, and for failing to provide adequate notice of precisely what information was accessed and stolen.

12. Maximus breached its duties to Plaintiffs and Class Members by maintaining Plaintiffs' and the Class Members' Private Information in a negligent and reckless manner.

13. Upon information and belief, the means of the Data Breach and potential risk for improper disclosure of Plaintiffs' and Class Members' Private Information were known and foreseeable to Maximus. Thus, Maximus was on notice that failing to take steps necessary to secure the Private Information from those risks left the Private Information in a dangerous and vulnerable condition.

14. Maximus and its employees failed to properly monitor the computer network and systems housing the Private Information.

15. Had Maximus properly monitored its property and that of its third-party contractor, it would have discovered the intrusion sooner or been able to wholly prevent it.

16. Exacerbating an already devastating privacy intrusion, Plaintiffs' and Class Members' identities are now at a heightened risk of exposure because of Maximus's negligent

conduct since the Private Information that Maximus collected and stored is now in the hands of data thieves.

17. Armed with the Private Information accessed in the Data Breach, data thieves can now use the PII and PHI obtained from Maximus to commit a variety of crimes, including credit/debit card fraud, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based upon their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

18. As a direct result of the Data Breach, Plaintiffs and Class Members have suffered fraud and will continue to be exposed to a heightened and imminent risk of fraud and identity theft, potentially for the rest of their lives. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

19. Plaintiffs and Class Members may also incur out-of-pocket costs for purchasing credit monitoring services, credit freezes, credit reports, and other protective measures to deter and detect identity theft.

20. As a direct and proximate result of the Data Breach and subsequent exposure of their Private Information, Plaintiffs and Class Members have suffered, and will continue to suffer damages and economic losses in the form of lost time needed to take appropriate measures to avoid unauthorized and fraudulent charges, putting alerts on their credit files, and dealing with spam phone calls, letters, and emails received as a result of the Data Breach.

21. Plaintiffs and Class Members have suffered, and will continue to suffer, an invasion of their property interest in their own PII and PHI such that they are entitled to damages from Maximus for unauthorized access to, theft of, and misuse of their Private Information. These harms are ongoing, and Plaintiffs and Class Members will suffer from future damages associated with the unauthorized use and misuse of their Private Information as thieves will continue to use the information to obtain money and credit in their names for several years.

22. Plaintiffs seek to remedy these harms on behalf of all similarly situated individuals whose Private Information was accessed via and/or compromised by Maximus during the Data Breach.

II. PARTIES

A. Plaintiffs

23. Plaintiff Clifford Beers ("Mr. Beers") is a resident of Leominster, Massachusetts and a citizen of Massachusetts. Mr. Beers learned of the Maximus Data Breach through a letter sent by Maximus and the Centers for Medicare & Medicaid Services to him via mail on July 28, 2023.

24. Plaintiff Wade Nugent ("Mr. Nugent") is a resident of Leitchfield, Kentucky and a citizen of Kentucky. Mr. Nugent learned of the Maximus Data Breach through a letter sent by Maximus and the Centers for Medicare & Medicaid Services to him via mail on July 28, 2023.

B. Defendants

25. Defendant Maximus, Inc. is a corporation organized under the laws of Virginia with its principal place of business in McLean, Virginia.

26. Defendant Maximus Federal Services, Inc. is a corporation organized under the laws of Virginia with its principal place of business in McLean, Virginia. Maximus Federal Services, Inc. is a wholly-owned subsidiary of Maximus, Inc.

III. JURISDICTION AND VENUE

27. This Court has subject-matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. §1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, consists of putative class membership of greater than 100 members, and is a class action in which some of the members of the Class, including Plaintiffs, are citizens of states different than that of Defendants.

28. This Court has personal jurisdiction over Defendants because their principal places of business are in Virginia.

29. Venue is proper in this Court pursuant to 28 U.S.C. §1391 because Defendants reside in this District, a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in, was directed to, and/or emanated from this District, and Defendants conduct substantial business in this District.

IV. STATEMENT OF FACTS

A. Defendant Maximus's Business

30. Touting itself as the "market leader in health services," Maximus was founded in 1975 and is a global company with approximately 39,500 employees that describes itself as "dedicated to helping governments on four continents to administer their citizen-facing programs."[4]

[4] Maximus, Inc. (Form 10-Q) (Aug. 3, 2023).

31. Maximus conducts its business operations through three segments: (1) U.S. Federal Services, (2) U.S. Services, and (3) Outside the U.S. Maximus, Inc.'s wholly-owned subsidiary MFSI contracts with U.S. Federal Government Agencies to provide services including the management and administration of government programs. This includes a contract with the Centers for Medicare & Medicaid Services ("CMS") to run its health insurance eligibility appeals process.[5] Maximus manages 70% of all Medicaid and CHIP beneficiary enrollments nationwide.[6] Maximus claims to have over 100 contracts in the United States, completing 1 million benefit appeals annually for government services, including eligibility, health, disability, and workers' compensation.[7] Maximus has served 52 million Medicaid and CHIP beneficiaries and operated 72 state and local health programs.[8] Through these contracts, Maximus cumulatively possesses and stores the PII and PHI of millions of people in its databases.

B. The Collection of Plaintiffs' and Class Members' Private Information is Central to Maximus's Business

32. In order for Maximus to offer its contracted services to government entity clients, the government entity clients were required to transfer possession of user PII and PHI to Maximus.

33. Through the possession and utilization of Plaintiffs' and Class Members' Private Information, Maximus assumed duties owed to Plaintiffs and Class Members regarding their Private Information. Therefore, Maximus knew or should have known that it was responsible for

[5] CMS provides health coverage to more than 100 million people through Medicare, Medicaid, CHIP, and the Health Insurance Marketplace.

[6] Health and Wellness, Maximus, Inc., https://maximus.com/health-and-wellness (last visited Aug. 17, 2023).

[7] *Id.*

[8] *Id.*

safeguarding Plaintiffs' and Class Members' Private Information from unauthorized access and criminal misuse.

34. Maximus has publicly touted its cybersecurity abilities, noting that its Technology and Consulting Services division's core capabilities include "deliver[ing] full spectrum cybersecurity services, including cyber engineering and operations, digital forensics, and incident response."[9]

35. Indeed, through Maximus's Privacy Statement, Maximus communicated the following:

> "Maximus uses various technological and procedural security measures in order to protect the personal information we collect through the Site from loss, misuse, alteration or destruction. We have documented Information Security & Privacy policies to address data protection. We regularly provide information security and privacy awareness training to our employees."[10]

36. Further, Maximus owed a duty to Plaintiffs and Class Members to perform due diligence on the subcontractors and service vendors who receive Private Information from Maximus. Maximus has even acknowledged that the company is required to "perform appropriate due diligence on [its] subcontractors and teaming partners."

37. The circumstances of the Data Breach suggest that Maximus utterly failed to conduct sufficient due diligence on its subcontractor, Progress Software, whose file transfer application, MOVEit, was the conduit for the Data Breach.[11] This failure is demonstrated through Maximus's extensive use of vulnerable file transfer protocol software, and both Progress

[9] Maximus, Inc. (Form 10-K) (Nov. 22, 2022).

[10] Privacy Statement, Maximus, Inc. (last visited Aug. 17, 2023).

[11] Maximus, Inc. (Form 10-K) (Nov. 22, 2022).

Software's delayed notification to Maximus of the vulnerability in its system and subsequent cyberattack, and the resulting breach of Plaintiffs' and Class Members' PII and PHI.

38. Plaintiffs and Class Members relied on Maximus to keep their Private Information secure and safeguarded for authorized purposes. Maximus owed a duty to Plaintiffs to secure their Private Information as such, and ultimately breached that duty.

C. The Data Breach

39. On or around May 27, 2023, a cyber attacker targeted a "critical zero-day vulnerability" in the Progress Software file transfer application, MOVEit, utilized by Maximus for internal and external file sharing purposes.[12] The Russia-linked ransomware group CL0P has since claimed responsibility for the cyberattack.[13]

40. On July 28, 2023, Maximus and CMS sent joint notice to Plaintiffs informing them of the Data Breach. In the Notice, Maximus claimed that it first detected unusual activity on May 30, 2023—three days into the cyberattack. Maximus claims that it began to investigate the Data Breach and stopped all use of the MOVEit application early on May 31, 2023. Maximus notified CMS of the incident on June 2, 2023.

41. In the July 28, 2023 joint notice, Maximus notified Plaintiffs and Class Members that their PII and PHI had been exposed, and therefore compromised, in the attack, including:

i. Name;

ii. Social Security Number or Individual Taxpayer Identification Number;

---

[12] Maximus, Inc. (Form 8-K) (July 26, 2023).

[13] *#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

iii. Date of Birth;

iv. Mailing Address;

v. Telephone Number and Fax Number;

vi. Email Address;

vii. Medicare Beneficiary Identifier (MBI) or Health Insurance Claim Number (HICN);

viii. Driver's License Number and State Identification Number;

ix. Medical History/Notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.);

x. Healthcare Provider and Prescription Information;

xi. Health Insurance Claims and Prescription Information;

xii. Health Insurance Claims and Policy/Subscriber Information; and

xiii. Health Benefits & Enrollment Information.

42. Maximus has yet to inform millions of individuals of the Data Breach. This has resulted in Class Members suffering harm they otherwise may have been able to avoid had Maximus announced and sent notice of the Data Breach sooner.

43. Maximus's Notice was therefore untimely and woefully deficient, failing to provide basic details concerning the Data Breach, including, but not limited to, how unauthorized parties accessed the third-party MOVEit software, whether the information was encrypted or otherwise protected, whether the breach was a system-wide breach, and how many people were affected by the Data Breach.

44. Given the intentional and criminal nature of the cybersecurity attack, Plaintiffs' and Class Members' Private Information is now for sale to criminals on the dark web; meaning unauthorized parties have accessed and viewed Plaintiffs' and Class Members' unencrypted,

unredacted Private Information, including names, dates of birth, billing and insurance information, medical records, diagnosis and prescription information, Social Security numbers, driver's licenses, and more.

D. Plaintiffs' Experiences Following the Data Breach

Clifford Beers

45. Mr. Beers has been a Medicare beneficiary since October 2013.

46. On multiple occasions, Mr. Beers has been required to provide his Private Information to Maximus, directly or indirectly, as a condition of applying for and receiving Medicare services.

47. Mr. Beers received a Data Breach Notice informing him of the Data Breach in July 2023.

48. Thereafter, Mr. Beers spent time taking action to mitigate the impact of the Data Breach after he received the Data Breach Notice. This effort included checking his bank accounts and other online accounts, examining his credit score, and researching the potential impact of the Data Breach, all as a result of his Private Information being exposed in the Data Breach. Mr. Beers intends to spend additional time and effort taking steps to protect his Private Information in the future. Because of the Data Breach, Mr. Beers spent valuable time he otherwise would have spent on other obligations.

49. Moreover, Mr. Beers spent this time at Maximus's direction. In the Data Breach Notice Mr. Beers received, Maximus encouraged Mr. Beers to spend time mitigating his losses by "reviewing [his] financial statements and accounts for signs of suspicious transactions and activities" and to "remain vigilant."

50. As a result of the Data Breach, Mr. Beers has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach. This is time Mr. Beers otherwise would have spent performing other activities.

51. In addition, Mr. Beers has suffered and will continue to suffer emotional distress as a result of the Data Breach, and has increased concerns for the loss of his privacy and the release of his protected health information, which he would not have suffered had Maximus implemented the necessary and proper safeguards to protect Plaintiffs' and Class Members' Private Information from theft.

52. The Private Information that was accessed in the Data Breach was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and foreseeable that Mr. Beers would take, and continue to take, necessary measures to protect his Private Information.

53. Mr. Beers has a continuing interest in ensuring that his Private Information, which, upon information and belief, remain in Maximus's possession, is protected and safeguarded from further and future breaches.

54. Mr. Beers suffered actual injury in the form of damages to and loss of potential value of his Private Information—a form of intangible property that Mr. Beers entrusted to Maximus for the purpose of receiving Medicare services, which was compromised in, and as a result, of the Data Breach.

55. Mr. Beers has also suffered actual injury in the form of:

i. Lost time by having to deal with all the consequences of the Data Breach, including reviewing and monitoring his bank accounts and other online accounts and researching the impacts of the Data Breach; and

ii. Dealing with a wave of scammer telephone calls and text messages—all as a result of his Private Information being exposed in the Data Breach. This is time Mr. Beers otherwise would have spent performing other activities or leisurely events for the enjoyment of life.

56. As a result of the Data Breach, Mr. Beers will continue to be at heightened risk for financial fraud, medical fraud and identity theft, and the attendant damages, for years to come.

Wade Nugent

57. Mr. Nugent has been a Medicare beneficiary for 13 years.

58. On multiple occasions, Mr. Nugent has been required to provide his Private Information to Maximus, directly or indirectly, as a condition of receiving Medicare services.

59. Mr. Nugent received a Data Breach Notice informing him of the Data Breach in July 2023.

60. Thereafter, Mr. Nugent spent time taking action to mitigate the impact of the Data Breach after he received the Data Breach Notice. This effort included checking his bank accounts and other online accounts, examining his credit score, and researching the potential impact of the Data Breach, all as a result of his Private Information being exposed in the Data Breach. Mr. Nugent intends to spend additional time and effort taking steps to protect his Private Information in the future. Because of the Data Breach, Mr. Nugent spent valuable time he otherwise would have spent on other obligations.

61. Moreover, Mr. Nugent spent this time at Maximus's direction. In the Data Breach Notice Mr. Nugent received, Maximus encouraged Mr. Nugent to spend time mitigating his losses by "reviewing [his] financial statements and accounts for signs of suspicious transactions and activities" and to "remain vigilant."

62. As a result of the Data Breach, Mr. Nugent has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach. This is time Mr. Nugent otherwise would have spent performing other activities.

63. In addition, Mr. Nugent has suffered and will continue to suffer emotional distress as a result of the Data Breach, and has increased concerns for the loss of his privacy and the release of his protected health information, which he would not have suffered had Maximus implemented the necessary and proper safeguards to protect Plaintiffs' and Class Members' Private Information from theft.

64. The Private Information that was accessed in the Data Breach was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and foreseeable that Mr. Nugent would take, and continue to take, necessary measures to protect his Private Information.

65. Mr. Nugent has a continuing interest in ensuring that his Private Information, which, upon information and belief, remain in Maximus's possession, is protected and safeguarded from further and future breaches.

66. Mr. Nugent suffered actual injury in the form of loss of potential value of his Private Information—a form of intangible property that Mr. Nugent entrusted to Maximus for the purpose of receiving Medicare services, which was compromised in, and as a result, of the Data Breach.

67. Mr. Nugent has also suffered actual injury in the form of lost time by having to deal with all the consequences of the Data Breach, including reviewing and monitoring his bank accounts and other online accounts and researching the impacts of the Data Breach—all as a result of his Private Information being exposed in the Data Breach. This is time Mr. Nugent otherwise would have spent performing other activities or leisurely events for the enjoyment of life.

68. As a result of the Data Breach, Mr. Nugent will continue to be at heightened risk for financial fraud, medical fraud and identity theft, and the attendant damages, for years to come.

E. The Healthcare Sector Is Particularly Susceptible to Cyberattacks

69. Maximus was or should have been on notice that the Federal Bureau of Investigation ("FBI") has been concerned about data security in the healthcare sector. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "'[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII).'"[14]

70. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[15]

[14] Jim Finkle, *FBI warns healthcare firms that they are targeted by hackers*, REUTERS (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

[15] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (emphasis omitted).

71. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[16] In 2022, 1,802 data compromises were reported that impacted over 422 million victims—marking a 42% increase in the number of victims impacted since 2021.[17] That upward trend continues.

72. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[18] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[19] Almost 50% of the victims lost their healthcare coverage as a result of the incident, while nearly thirty percent said their insurance premiums went up after the event. Forty percent of the customers were never

[16] Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout, CISION PR NEWSWIRE (Jan. 19, 2017), https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html.

[17] 2022 Annual Data Breach Report, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited Aug. 17, 2023).

[18] 2018 End-of-Year Data Breach Report, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINALWEB-V2-2.pdf (last visited Aug. 17, 2023).

[19] Elinor Mills, Study: Medical identity theft is costly for victims, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[20]

73. Healthcare related data breaches also come at a cost to the breached entities. According to IBM's 2023 Cost of a Data Breach Report, the healthcare sector reported the highest data breach costs for the thirteenth year in a row in 2023—increasing 8.2% from $10.10 million in 2022 to $10.93 million in 2023.[21] This cost should only further incentivize service providers to both invest in and implement reasonable and adequate security measures in order to avoid financial repercussions in the event of a breach.

74. Healthcare related data breaches have continued to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82% of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[22]

> Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information (PII) for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.[23]

---

[20] *Id.*

[21] Cost of a Data Breach Report 2023, IBM, *available at* https://www.ibm.com/reports/data-breach.

[22] 2019 HIMSS Cybersecurity Survey, HIMSS, https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited Aug. 17, 2023).

[23] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, CHIEF HEALTHCARE EXEC. (Apr. 4, 2019), https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

75. Critically, this is not the first data breach suffered by individuals going through Maximus to receive government services. In May 2021, Ohio Medicaid stated that its contractor, Maximus, suffered a data breach in which an application containing Ohio Medicaid credential and licensing data was accessed without authorization by an unknown third party.[24] Maximus reported the breach to the Maine Attorney General as impacting 334, 690 individuals in multiple U.S. states.

76. Given Maximus's work centered on accessing and maintaining sensitive PII and PHI, and given its previous experience with a data breach, Maximus knew or reasonably should have known the importance of implementing reasonable and adequate practices and procedures in order to safeguard the PII and PHI entrusted to it by individuals receiving government services.

77. As entities both contracting with healthcare service providers and handling, storing, and safeguarding PII and PHI, Maximus knew, or reasonably should have known, the importance of safeguarding the Private Information entrusted to it, and of the foreseeable consequences if its data security systems were breached. This duty extends to Maximus's obligations to safeguard PII and PHI shared with subcontractors and service vendors who received Private Information from Maximus. Maximus failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

i. The Value of Private Information and the Effects of Unauthorized Disclosure

78. At all relevant times, Maximus was well aware that the Private Information it collects from Plaintiffs and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

[24] *Maximus Reports Breach Affecting 334,000 Medicaid Healthcare Providers*, THE HIPAA JOURNAL (June 24, 2021), https://www.hipaajournal.com/maximus-reports-breach-affecting-334000-medicaid-healthcare-providers/.

79. Private Information is a valuable commodity to cyber attackers. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[25] Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground websites, commonly referred to as the dark web.

80. While credit card information and associated PII can sell for as little as $1-$2 on the black market, PHI can sell for as much as $363.[26]

81. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

82. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "'Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery,'" reported Pam Dixon, executive director of World Privacy Forum. "'Victims often experience

[25] *What to Know About Identify Theft*, Fed. Trade Comm'n, https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Aug. 17, 2023).

[26] *Data Breaches: In the Healthcare Sector,* Ctr. for Internet Sec., https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited Aug. 17, 2023).

financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities.'"[27]

83. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.[28]

84. The ramifications of Maximus's failures to keep Plaintiffs' and Class Members' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

85. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

86. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[29] This gives thieves ample time to seek multiple treatments under the victim's name. And 40% of consumers found out they were a victim of

---

[27] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, Kaiser Health News (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.

[28] *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIV. (Apr. 8, 2014), https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf.

[29] *See Medical ID Theft Checklist*, IdentityForce https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited Aug. 17, 2023).

medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[30]

87. As a company contracting with public health sector government entities, Maximus knew, or reasonably should have known, the importance of safeguarding Plaintiffs' and Class Members' Private Information entrusted to it, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach. Maximus failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

i. Maximus's Conduct Violates HIPAA

88. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[31]

89. Maximus is a covered entity under HIPAA and is therefore required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

---

[30] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), Experian (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[31] *What is Considered Protected Health Information Under HIPAA?*, HIPAA J. (Jan. 1, 2023), https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.

90. Title II of HIPAA contains the Administrative Simplification provisions. 42 U.S.C. §§1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Maximus failed to safeguard. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

91. The HIPAA Breach Notification Rule, 45 CFR §§164.400-414, also required Maximus to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of a breach."[32]

92. Based on information and belief, Maximus's Data Breach resulted from a combination of insufficiencies that demonstrate Maximus failed to comply with safeguards mandated by HIPAA regulations and industry standards. Maximus's security failures include, but are not limited to, the following:

a. Failing to ensure the confidentiality and integrity of electronic protected health information that Maximus receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);

b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

[32] *Breach Notification Rule*, U.S. Dep't of Health & Human Servs., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Aug. 17, 2023) (emphasis added).

c. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §164.308(a)(1);

d. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

e. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. §164.306(a)(2);

f. Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

g. Failing to ensure compliance with HIPAA security standard rules by its workforce in violation of 45 C.F.R. §164.306(a)(94);

h. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

i. Failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out its functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

j. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. §164.530(c).

i. Maximus Failed to Comply with FTC Guidelines

93. Maximus was also prohibited by the Federal Trade Commission Act ("FTCA") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTCA.[33]

94. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[34]

95. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[35] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.

---

[33] *See, e.g.*, *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407 (E.D. Va. 2020) (citing *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015)).

[34] *Start With Security: A Guide for Business*, Fed. Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Aug. 17, 2023).

[35] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Aug. 17, 2023).

96. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

97. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. §45. Orders resulting from these actions further clarify the measures businesses must take to meet its data security obligations.

98. Maximus failed to properly implement basic data security practices. Maximus's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. §45.

99. Maximus was fully aware of its obligations to protect the Private Information of Plaintiffs and Class Members because of its position as a service provider whose business centers on the collection, storage, and safeguarding of PII and PHI. Maximus was also aware of the significant repercussions that would result from its failure to make good on those obligations.

i. Cyber Criminals Have and Will Continue to Use Plaintiffs' and Class Members' PII and PHI for Nefarious Purposes

100. Plaintiffs' and Class Members' highly sensitive PII and PHI is of great value to cybercriminals, and the data stolen in the Data Breach can be used in a variety of ways for criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune and stolen information. The cybercriminals' motives for the Data Breach were purely nefarious and

malicious in nature: their one goal was to access systems, including Maximus's systems, in order to obtain valuable PII and PHI to sell on the dark web.

101. Every year, identity theft causes tens of billions of dollars of losses to victims in the United States.[36] For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[37] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

102. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.

103. These risks are both certainly impending and substantial. As the FTC has reported, if cyber attackers get access to PII, they will use it.[38]

104. Cyber attackers may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

---

[36] *Facts + Statistics: Identity Theft and Cybercrime*, INS. INFO. INSTITUTE, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Aug. 17, 2023) (discussing Javelin Strategy & Research's report *2018 Identity Fraud: Fraud Enters a New Era of Complexity*).

[37] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, CREDIT.COM (Nov. 2, 2017), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[38] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[39]

105. If cyber criminals manage to access PII, health insurance information, and other personally sensitive data, as is the case with this Data Breach, there is no limit to the amount of fraud to which Maximus may have exposed Plaintiffs and Class Members.

i. Plaintiffs and Class Members Suffered Damages

106. The ramifications of Maximus's failures to keep Plaintiffs' and Class Members' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[40]

107. In addition to their obligations under state laws and regulations, Maximus owed a common law duty to Plaintiffs and Class Members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties. This duty extends to Maximus's obligations to safeguard PII and PHI shared with subcontractors and service vendors who received Private Information from Maximus, and to conduct ongoing, robust due diligence into such subcontractors and service vendors prior to contracting and throughout any relationship.

---

[39] Stolen Laptops Lead to Important HIPAA Settlements, U.S. DEP'T OF HEALTH & HUMAN SERVS. (Apr. 22, 2014), https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

[40] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

108. Maximus further owed and breached its duties to Plaintiffs and Class Members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems. Instead of implementing such processes and specifications, Maximus allowed the Data Breach to go undetected for three days before recognizing unusual activity.

109. As a direct result of Maximus's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, cyber attackers were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse to Plaintiffs' and Class Members' Private Information as detailed above, and Plaintiffs are now at a heightened risk of identity theft and fraud.

110. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

111. Other risks of identity theft include loans opened in the name of the victim, medical services billed in their name, utility bills opened in their name, tax return fraud, and credit card fraud.

112. Plaintiffs and Class Members did not receive the full benefit of the bargain for received healthcare and other services. As a result, Plaintiffs and Class Members were damaged in an amount at least equal to the difference in the value of the government services with data security protection they paid for and the services they received without the data security protection.

113. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information has lost potential value.

114. The Private Information belonging to Plaintiffs and Class Members is private, private in nature, and was left inadequately protected by Maximus who did not obtain Plaintiffs' or Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standards.

115. The Data Breach was a direct and proximate result of Maximus's failure to: (a) properly safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

116. Maximus had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect patient data.

117. Had Maximus remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into their systems and, ultimately, the theft of Plaintiffs' and Class Members' Private Information.

118. As a direct and proximate result of Maximus's wrongful actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

119. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "[r]esolving the problems caused by identity theft [could] take more than a year for some victims."[41]

120. Maximus's failures to adequately protect Plaintiffs' and Class Members' Private Information has resulted in Plaintiffs and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money. Rather than assist those affected by the Data Breach, Maximus is putting the burden on Plaintiffs and Class Members to discover possible fraudulent activity and identity theft.

121. As a result of Maximus's failures to prevent the Data Breach, Plaintiffs and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their Private Information;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

d. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fail to undertake appropriate measures to protect the Private Information in their possession;

[41] Erika Harrell, & Lynn Langton, *Victims of Identity Theft, 2012*, U.S. DEP'T OF JUST., OFF. OF JUST. PROGRAMS BUREAU OF JUST. STATS. (Dec. 2013), https://www.bjs.gov/content/pub/pdf/vit12.pdf.

e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and

f. Anxiety and distress resulting from fear of misuse of their medical information.

124. In addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

i. Maximus's Delay in Identifying & Reporting the Breach Caused Additional Harm

122. It is axiomatic that:

> The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act.[42]

123. Indeed, once a data breach has occurred:

> [o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers.
>
> "If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves. . . . "[43]

[42] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, BUSINESS WIRE (Feb. 1, 2017), https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million.

[43] Allen St. John, *The Data Breach Next Door*, CONSUMER REPORTS, (Jan. 31, 2019), https://www.consumerreports.org/data-theft/the-data-breach-next-door/.

124. Although their Private Information was improperly exposed on or before May 27, 2023, Maximus did not notify Plaintiffs and Class Members until almost two months following the Data Breach. Additionally, millions of Class Members have not yet been notified of the Data Breach—depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

125. As a result of Maximus's delay in detecting and notifying individuals of the Data Breach, the risk of fraud for Plaintiffs and Class Members has been driven even higher.

CLASS ALLEGATIONS

126. Plaintiffs bring this class action on behalf of themselves and all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

127. The Class that Plaintiffs seek to represent is defined as follows:

> **All individuals in the United States whose Private Information was compromised in the Data Breach.**

128. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers, and directors, current or former employees, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

129. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

130. Numerosity, Fed R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all members is impracticable. Defendants have identified at least 14.5 to 17.5 million individuals

whose Private Information may have been improperly accessed and compromised in the Data Breach.

131. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

i. Whether and when Defendants actually learned of the Data Breach and whether their response was adequate;

ii. Whether Defendants owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining Class Members' Private Information;

iii. Whether Defendants breached that duty;

iv. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiffs' and Class Members' Private Information;

v. Whether Defendants acted negligently in connection with the monitoring and/or protecting of Plaintiffs' and Class Members' Private Information;

vi. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class Members' Private Information secure and prevent loss or misuse of that Private Information;

vii. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

viii. Whether Defendants caused Plaintiffs' and Class Members' damages;

ix. Whether Defendants violated the law by failing to promptly notify Class Members that their Private Information had been compromised;

x. Whether Plaintiffs and the other Class Members are entitled to actual damages, extended credit monitoring, and other monetary relief; and

xi. Whether Defendant violated common law and statutory claims alleged herein.

132. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members, because all had their Private Information compromised as a result of the Data Breach, due to Defendants' misfeasance.

133. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect the Class uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

134. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex consumer class action litigation, and Plaintiffs intend to prosecute this action vigorously.

135. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the

controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

136. The nature of this action and the nature of laws available to Plaintiffs and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and the Class for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since Defendants would be able to exploit and overwhelm the limited resources of the Class with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

137. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

138. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

139. Unless a Class-wide injunction is issued, Plaintiffs and Class Members remain at risk that Defendants will continue to fail to properly secure the Private Information of Plaintiffs and Class Members resulting in another data breach, continue to refuse to provide proper notification to Class Members regarding the Data Breach, and continue to act unlawfully as set forth in this Class Action Complaint.

140. Defendants acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

141. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendants breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendants failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendants failed to implement and maintain reasonable and adequate security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether Class Members are entitled to actual damages, additional credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

142. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

143. Plaintiffs and Class Members were required to submit their Private Information in order to receive government services.

144. Defendants knew, or should have known, of the risks inherent in collecting and storing the Private Information of Plaintiffs and Class Members.

145. As described above, Defendants owed duties of care to Plaintiffs and Class Members whose Private Information had been entrusted with Defendants.

146. Defendants breached their duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

147. Defendants acted with wanton disregard for the security of Plaintiffs' and Class Members' Private Information. Defendants knew or reasonably should have known that they had inadequate data security practices to safeguard such information, and Defendants knew or reasonably should have known that data thieves were attempting to access databases containing PII and PHI, such as those of Defendants.

148. A "special relationship" exists between Defendants and Plaintiffs and Class Members. Defendants entered into a "special relationship" with Plaintiffs and Class Members

because Defendants collected the Private Information of Plaintiffs and the Class Members—information that Plaintiffs and the Class Members were required to provide in order to receive government services.

149. But for Defendants' wrongful and negligent breaches of the duties owed to Plaintiffs and the Class Members, Plaintiffs and the Class Members would not have been injured.

150. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breaches of their duties. Defendants knew or reasonably should have known they were failing to meet their duties, and that Defendants' breaches of such duties would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

151. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

152. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

153. Pursuant to the FTCA (15 U.S.C. §45), Defendants had a duty to provide fair and adequate data security practices to safeguard Plaintiffs' and Class Members' Private Information.

154. Pursuant to HIPAA (42 U.S.C. §§1302d, *et seq*.), Defendants had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

155. Defendants breached their duties to Plaintiffs and Class Members under the FTCA (15 U.S.C. §45) and HIPAA (42 U.S.C. §§1302d, *et seq*.), by failing to provide fair, reasonable,

or adequate data security practices to safeguard Plaintiffs' and Class Members' Private Information.

156. Defendants' failures to comply with applicable laws and regulations constitutes negligence *per se*.

157. But for Defendants' wrongful and negligent breaches of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

158. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breaches of their duties. Defendants knew or reasonably should have known that they were failing to meet their duties, and that Defendants' breaches would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

159. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

160. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

161. Plaintiffs and Class Members entered into an implied contract with Defendants when they sought or obtained services from government entities, in exchange for which they were required to provide their Private Information. The Private Information provided by Plaintiffs and Class Members to Defendants was governed by and subject to Defendants' privacy duties and policies.

162. Defendants agreed to safeguard and protect the Private Information of Plaintiffs and Class Members and to timely and accurately notify Plaintiffs and Class Members in the event that their Private Information was breached or otherwise compromised.

163. Plaintiffs and Class Members entered into the implied contracts with the reasonable expectation that Defendants' data security practices and policies were reasonable and consistent with industry standards. Plaintiffs and Class Members believed that Defendants would use part of the monies paid to Defendants under the implied contracts to fund adequate and reasonable data security practices.

164. Plaintiffs and Class Members would not have entrusted their Private Information to Defendants in the absence of the implied contract or implied terms between Plaintiffs and Class Members and Defendants. The safeguarding of the Private Information of Plaintiffs and Class Members and prompt and sufficient notification of a breach involving Private Information was critical to realize the intent of the parties.

165. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendants.

166. Defendants breached their implied contracts with Plaintiffs and Class Members to protect Plaintiffs' and Class Members' Private Information when they: (1) failed to have data security practices in place to protect that information; (2) disclosed that information to unauthorized third parties; and (3) failed to provide timely and accurate notice that their Private Information was compromised as a result of the Data Breach.

167. As a direct and proximate result of Defendants' breaches of implied contract, Plaintiffs and Class Members have suffered damages.

COUNT IV
Breach of Third-Party Beneficiary Contract

(On behalf of Plaintiffs and the Class)

168. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

169. This Count is pleaded in the alternative to the breach of implied contract claim above (Count III).

170. Upon information and belief, Defendants entered into contracts with its government entity clients, to provide health and human services—including data security practices, procedures, and protocols sufficient to safeguard the Private Information of Plaintiffs and Class Members.

171. These contracts were made for the benefit of Plaintiffs and Class Members given the transfer of their Private Information to Defendants for maintenance, protection, and safeguarding was the objective of the contracting parties. Therefore, Plaintiffs and Class Members were direct and express beneficiaries of these contracts.

172. Defendants knew that a breach of these contracts with its government entity clients would harm Plaintiffs and Class Members.

173. Defendants breached the contracts with its government entity clients when they failed to utilize adequate data security practices to safeguard Plaintiffs' and Class Members' Private Information.

174. Plaintiffs and Class Members were harmed by Defendants' breaches in failing to use reasonable data security measures to safely maintain and protect Plaintiffs' and Class Members' Private Information.

175. Plaintiffs and Class Members are therefore entitled to damages in an amount to be determined at trial.

COUNT V
Unjust Enrichment

(On behalf of Plaintiffs and the Class)

176. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

177. This Count is pleaded in the alternative to the breach of implied contract claim above (Count III) and the breach of third-party beneficiary claim above (Count IV).

178. Plaintiffs and Class Members conferred a benefit on Defendants. Specifically, they provided Defendants with their Private Information—Private Information that has inherent value. In exchange, Plaintiffs and Class Members should have been entitled to Defendants' adequate storage and safeguarding of their Private Information.

179. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and Class Members.

180. Defendants benefitted from Plaintiffs' and Class Members' retained Private Information and used their Private Information for business purposes.

181. Defendants failed to store and safeguard Plaintiffs' and Class Members' Private Information. Had Plaintiffs and Class Members known that Defendants were unable to adequately store and safeguard their Private Information, they would not have applied for or received government services in the manner that they did. Thus, Defendants did not fully compensate Plaintiffs and Class Members for the value of their Private Information.

182. As a result of Defendants' failures, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between the government services with the adequate data privacy and security practices that Plaintiffs and Class Members bargained for, and the government services without adequate data privacy and security practices that they received.

183. Under principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendants failed to implement—or adequately implement—the data privacy and security practices that Plaintiffs and Class Members paid for and that were otherwise mandated by HIPAA regulations, federal, state, and local laws, and industry standards.

184. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received by Defendants.

185. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendants traceable to Plaintiffs and Class Members.

PRAYER FOR RELIEF

A. That the Court certify this action as a class action and certify the Class as proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are the proper class representative; and appoint Plaintiffs' Counsel as Class counsel;

B. That the Court grant permanent injunctive relief to prohibit Defendants from engaging in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiffs and members of the Class compensatory, consequential, and general damages in an amount to be determined at trial;

D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

E. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

F. That Plaintiffs be granted the declaratory relief sought herein;

G. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

H. That the Court award pre- and post-judgment interest at the maximum legal rate; and

I. That the Court grant all such other relief as it deems just and proper.

Dated: August 21 2023

Respectfully submitted,

/s/ Bernadette Armand
Bernadette Armand (Bar No. 81332)
DiCELLO LEVITT LLP
1101 17th Street, NW
Suite 1000
Washington, DC 20036
Tel.: (202) 975-2288
barmand@dicellolevitt.com

BERMAN TABACCO
Patrick T. Egan (*pro hac vice* forthcoming)
Christina L. Gregg (*pro hac vice* forthcoming)
One Liberty Square
Boston, MA 02109
Telephone: (617) 542-8300
pegan@bermantabacco.com
cgregg@bermantabacco.com

DiCELLO LEVITT LLP

Adam J. Levitt (*pro hac vice* forthcoming)
Amy E. Keller (*pro hac vice* forthcoming)
Ten North Dearborn St., Sixth Floor
Chicago, Illinois 60602
Tel.: (312) 214-7900
alevitt@dicellolevitt.com
akeller@dicellolevitt.com

Corban Rhodes (*pro hac vice* forthcoming)

485 Lexington Ave., 10th Floor
New York, NY 10017
Tel.: (646) 933-1000
crhodes@dicellolevitt.com

Justin Hawal (*pro hac vice* forthcoming)
8160 Norton Parkway
Mentor, Ohio 44060
Tel.: (440) 953-8888
jhawal@dicellolevitt.com

CERTIFICATE OF SERVICE

I hereby certify that on August 21, 2023 a copy of the foregoing was filed electronically. Service of this filing will be made on all ECF-registered counsel by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

/s/ Bernadette Armand